Sécurisation de l'intégration de l'annuaire LDAP avec Cisco Unified CallManager 4.x

Contenu

Introduction

Ce document examine ces questions :

- Améliorez la Sécurité de l'intégration de répertoire LDAP avec le Cisco Unified CallManager (CUCM) avec plusieurs étapes de configuration pour limiter des autorisations. Ces procédures

améliorent une installation existante et nouvelle de l'intégration de répertoire.
- L'accès et la Gestion du répertoire exigent un utilisateur spécial et le groupent. Des autorisations sont placées sur des objets de limiter l'utilisateur et le groupe dédiés, et l'intégration de répertoire est alors mise à jour (pour un existant installez) ou s'est terminée (pour un nouveau installez). En conclusion, l'intégration est vérifiée.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document est spécifique au Cisco Unified CallManager 4.x.

Ces étapes, qui sont affichées avec la Microsoft Active Directory (AD), peuvent également appliquer à d'autres Produits pris en charge de répertoire.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Pour l'intégration existante de répertoire

Suivez ces étapes pour une intégration existante de répertoire :

1. Créez un nouveau groupe, tel que le *groupe de répertoire CUCM*.
2. Placez les autorisations de groupe pour l'accès de répertoire.
3. Déplacez l'utilisateur de répertoire existant au nouveau groupe.
4. Retirez l'utilisateur du vieux groupe ; les membres peuvent seulement être du nouveau groupe.
5. Exécutez la vérification.

Pour l'installation existante sans compte dédié

Suivez ces étapes pour une intégration existante de répertoire où un compte dédié n'a pas été utilisé :

1. Créez un nouvel utilisateur, tel que le *gestionnaire de répertoire CUCM*.
2. Faites à l'utilisateur un membre du nouveau groupe seulement.
3. Modification CUCM pour utiliser le nouvel utilisateur ; modifiez le registre et le fichier d'ini.
4. Redémarrez Cisco Tomcat.
5. Changez le mot de passe du compte d'origine qui avait été utilisé.

6. Exécutez la vérification.

Pour une nouvelle installation

Suivez ces étapes pour une nouvelle installation de l'intégration de répertoire :

1. Créez un nouveau groupe, tel que le *groupe de répertoire CUCM*.
2. Placez les restrictions sur ce nouveau groupe.
3. Créez un nouvel utilisateur, tel que le *gestionnaire de répertoire CUCM*.
4. Mettez le nouvel utilisateur dans un groupe avec des privilèges d'administrateur, par exemple, des *admins de domaine*.
5. Utilisez le nouvel utilisateur quand vous installez le périphérique prêt à brancher.
6. Déplacez l'utilisateur au *groupe* de création récente de *répertoire CUCM*.
7. Placez le nouveau groupe en tant que groupe primaire pour l'utilisateur d'admin.
8. Retirez cet utilisateur du vieux groupe, qui doit plus n'être un membre de n'importe quel autre groupe.
9. Exécutez la vérification.

Vérification

Exécutez la vérification avec cette procédure :

1. Créez un nouvel utilisateur, *ccmtest*, dans le répertoire (sur le serveur de répertoire).
2. Vérifiez que l'utilisateur ccmtest est répertorié dans des utilisateurs CUCM.
3. Changez le PIN du ccmtest à la page de configuration utilisateur CUCM.
4. Assurez-vous que le champ est mis à jour dans le répertoire.
5. La modification ciscoCCNatCTIUseEnabled **pour rectifier** pour ccmtest dans le répertoire.
6. Confirmez que la case d'**utilisation d'application de l'enable CTI** est ccmtest vérifié dans CUCM.
7. L'utilisateur **ccmtest d'**effacement.
8. Assurez-vous que seulement les pièces voulues de l'arborescence sont visibles avec un navigateur de LDAP : nécessité ne pas pouvoir visualiser n'importe quoi en dehors de l'OU de l'unité organisationnelle (OU) ou des utilisateurs de Cisco.

Étapes détaillées

Remarque: Les noms qui sont utilisés ici pour le compte dédié et le groupe sont *gestionnaire de répertoire CUCM* et *groupe de répertoire CUCM*, respectivement, mais vous pouvez choisir différents noms.

Microsoft Active Directory de début (ADUC)

Choisissez le **Start > Programs > Administrative tools >** les **utilisateurs et les ordinateurs de Répertoire actif**.

Créez le nouveau groupe

Suivez ces étapes pour créer le nouveau groupe :

1. Cliquez avec le bouton droit le conteneur d'**utilisateurs**.
2. Choisissez **nouveau > groupe**.
3. Écrivez le `nom de groupe`, la `portée`, et le `type`, tel que le *groupe de répertoire CUCM, global*, et la *Sécurité*.
4. Cliquez sur **Next** (Suivant).
5. Cliquez sur **Finish** (Terminer).

Autorisations de set group pour le répertoire Access

On doit accorder le groupe ces droites :

```
Read/Write/Create all child objects/
   Delete all child objects on the Cisco OU
```

Ces droites doivent s'appliquer à cet objet et à tous les objets d'enfant.

```
Read privileges on the Users OU,
   Read/Write privileges on the ciscoatGUID,
   ciscoatUserProfile, and ciscoatUserProfileString
   attributes for all User objects.
```

Lecture/écriture réglés/créent des privilèges sur l'OU de Cisco

Suivez ces étapes pour placer la lecture/écriture/créez les privilèges sur l'OU de Cisco :

1. Cliquez avec le bouton droit le conteneur de **Cisco**.
2. Choisissez **Properties**.
3. Choisissez l'**onglet Sécurité**.
4. Cliquez sur **Advanced**.
5. Cliquez sur **Add….**
6. Écrivez le `groupe du répertoire CCM`.
7. Le positionnement **s'appliquent sur le** champ à **cet objet et à tous les objets d'enfant**.
8. Le contrôle **tiennent compte** de **a lu tout le Properties**.
9. Le contrôle **tiennent compte** de **écrivent tout le Properties**.
10. Le contrôle **tiennent compte** de **créent tous les objets d'enfant**.
11. Le contrôle **permettent** pour l'**effacement tous les objets d'enfant**.
12. Cliquez sur **OK**.

Placez les privilèges lus sur l'OU des utilisateurs

Suivez ces étapes pour placer des privilèges lus sur l'OU d'utilisateurs :

1. Cliquez avec le bouton droit le conteneur d'**utilisateurs**.
2. Choisissez **Properties**.
3. Choisissez l'**onglet Sécurité**.
4. Cliquez sur **Advanced**.
5. Cliquez sur **Add….**
6. Écrivez le `groupe du répertoire CCM`.
7. Le positionnement **s'appliquent sur le** champ aux objets utilisateurs.

8. Le contrôle **tiennent compte** de **a lu tout le Properties**.
9. Cliquez sur **OK**.

Placez les privilèges lecture/écriture sur des attributs de Cisco

Suivez ces étapes pour placer des privilèges lecture/écriture sur les attributs de Cisco :

1. Cliquez avec le bouton droit le conteneur d'**utilisateurs**.
2. Choisissez **Properties**.
3. Choisissez l'**onglet Sécurité**.
4. Cliquez sur **Advanced**.
5. Cliquez sur **Add….**
6. Écrivez le `groupe du répertoire CCM`.
7. Le positionnement **s'appliquent sur le** champ aux objets utilisateurs.
8. Le contrôle **tiennent compte du ciscoatGUID lu, a lu ciscoatUserProfile, ReadatUserProfileString**.
9. Le contrôle **tiennent compte du ciscoatGUID Write, écrivent ciscoatUserProfile, écrivent atUserProfileString**.
10. Cliquez sur **OK**.

Créez le nouvel utilisateur

Suivez ces étapes pour créer un nouvel utilisateur :

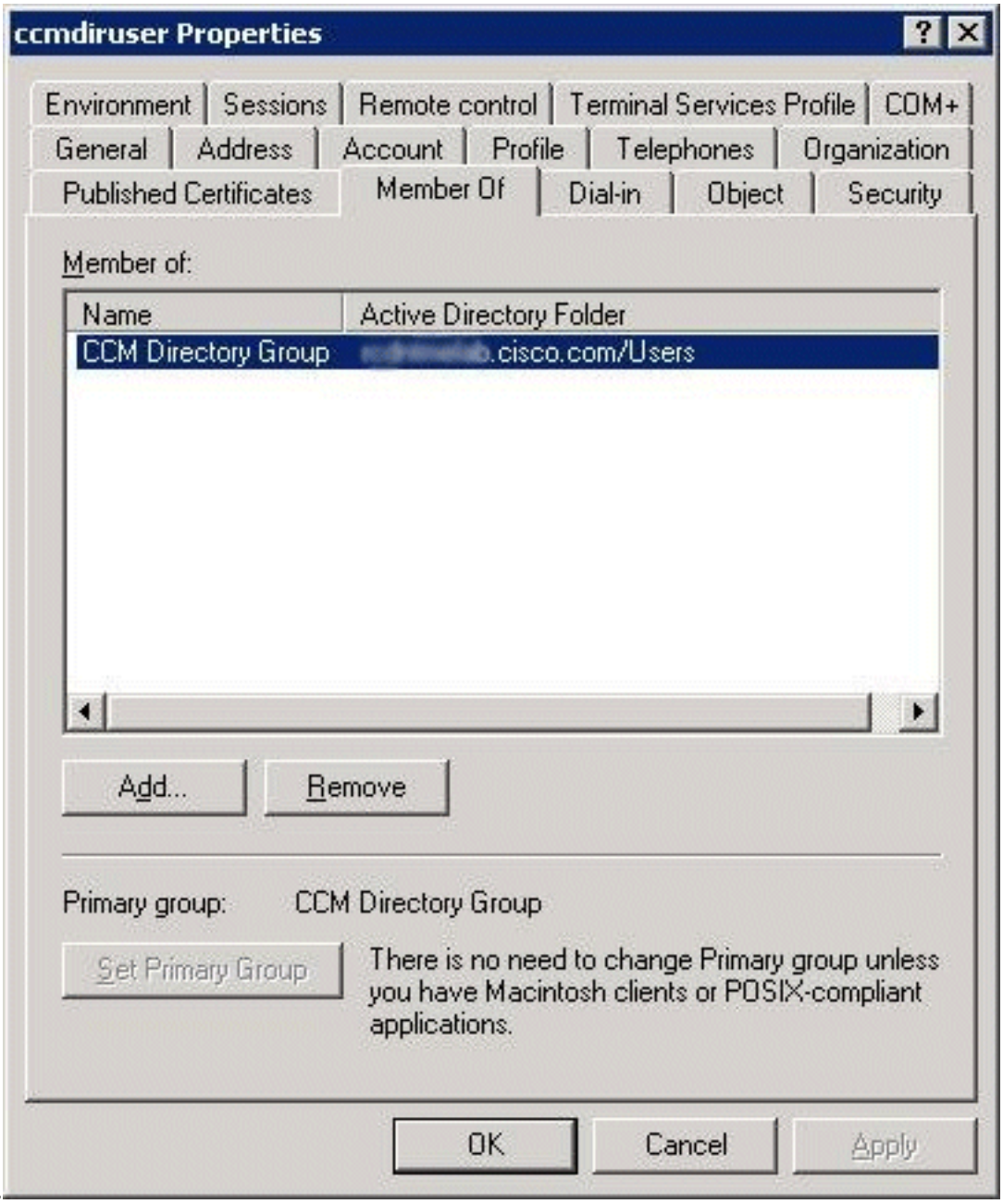
1. Cliquez avec le bouton droit le conteneur d'**utilisateurs**.
2. Choisissez **nouveau > utilisateur**.
3. Écrivez le **nom** et le nom de connexion, comme, *gestionnaire de répertoire CUCM, ccmdiruser*.
4. Complétez les champs de **mot de passe** et de **confirmation du mot de passe**.
5. Cochez le **mot de passe n'expire jamais**.
6. Cliquez sur **Next** (Suivant).
7. Cliquez sur **Finish** (Terminer).

Déplacez l'utilisateur au nouveau groupe et le retirez du vieux groupe

Suivez ces étapes pour déplacer l'utilisateur à un nouveau groupe et pour le retirer du vieux groupe :

1. Choisissez l'OU d'**utilisateurs**.
2. Cliquez avec le bouton droit le **ccmdiruser** et choisissez Properties.
3. Choisissez le **membre de l'**onglet.
4. Cliquez sur **Add….**
5. Écrivez le `groupe du répertoire CCM`.
6. Cliquez sur **OK**.
7. Choisissez le `groupe du répertoire CCM`.
8. **Groupe primaire réglé de** clic.
9. Choisissez le vieux groupe.

10. Le clic **retirent**.



Étape nécessaire trois pour changer CUCM pour utiliser le nouvel utilisateur

Trois étapes sont exigées pour changer CUCM pour utiliser le nouvel utilisateur :

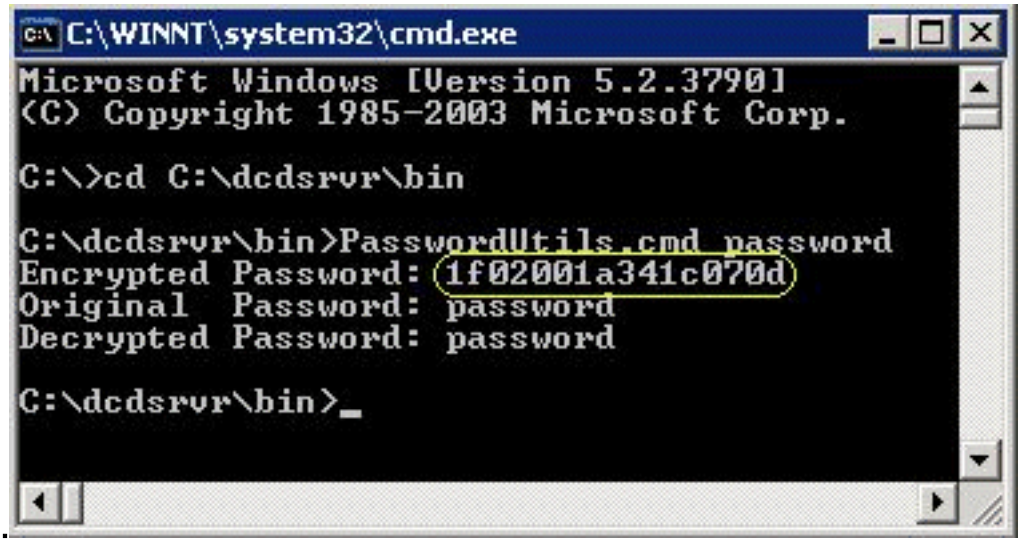
- Obtenez le mot de passe chiffré.
- Placez le compte et le mot de passe dans le registre.
- Placez le compte et le mot de passe dans le fichier d'initialisation de DC Directory.

Obtenez le mot de passe chiffré

Remarque: Bien que le mot de passe qui est utilisé ici soit ***mot de passe*** pour la démonstration, vous devez utiliser un mot de passe complexe à la place.

1. Choisissez **Start > Run**.
2. Écrivez le **cmd**.
3. Entrez dans le **cd C:\dcdsrvr\bin**.
4. Entrez le **mot de passe**

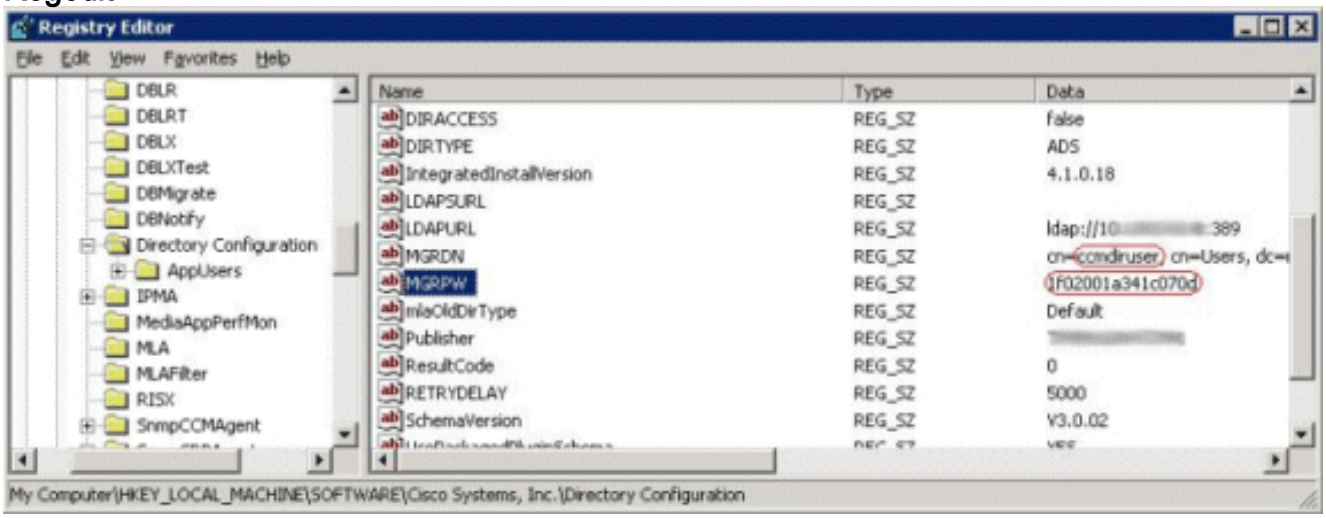
PasswordUtils.cmd.



Placez le compte et le mot de passe dans le registre

Attention : Si vous éditez la clé de registre fausse ou faites une erreur tandis que vous éditez le registre, votre système peut être inutilisable jusqu'à ce que vous répariez le registre. Vous devez sauvegarde votre registre avant que vous apportiez toutes les modifications. Assurez-vous que vous savez restaurer le registre de la sauvegarde avant que vous continuiez. Puisqu'une explication de la façon mettre à jour le registre de serveur est hors de portée de ce document, consultez votre documentation de système pour ces informations.

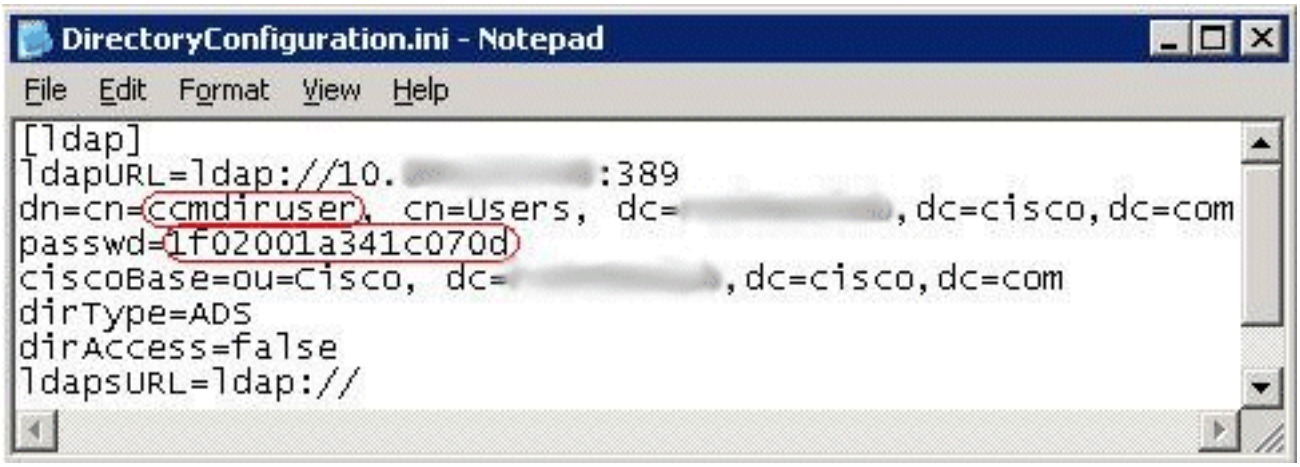
1. Choisissez **Start > Run**.
2. Écrivez le **regedit** et cliquez sur OK.
3. Parcourez au **\ \ HKEY_LOCAL_MACHINE \ logiciel \ Cisco Systems, Inc. \ configuration de répertoire** dans le registre.
4. Dans le volet de droite, double-cliquer la clé de registre **MGRDN**.
5. Changez l'utilisateur, par exemple, *administrateur > ccmdiruser*.
6. Double-cliquer la clé de registre **MGRPW**.
7. Changez le mot de passe chiffré avec la valeur obtenue de l'outil de **PasswordUtils**.
8. Quittez **Regedit**.



Placez le compte et le mot de passe dans le fichier d'ini de DC Directory

Suivez ces étapes pour placer le compte et le mot de passe dans le fichier d'ini de DC Directory :

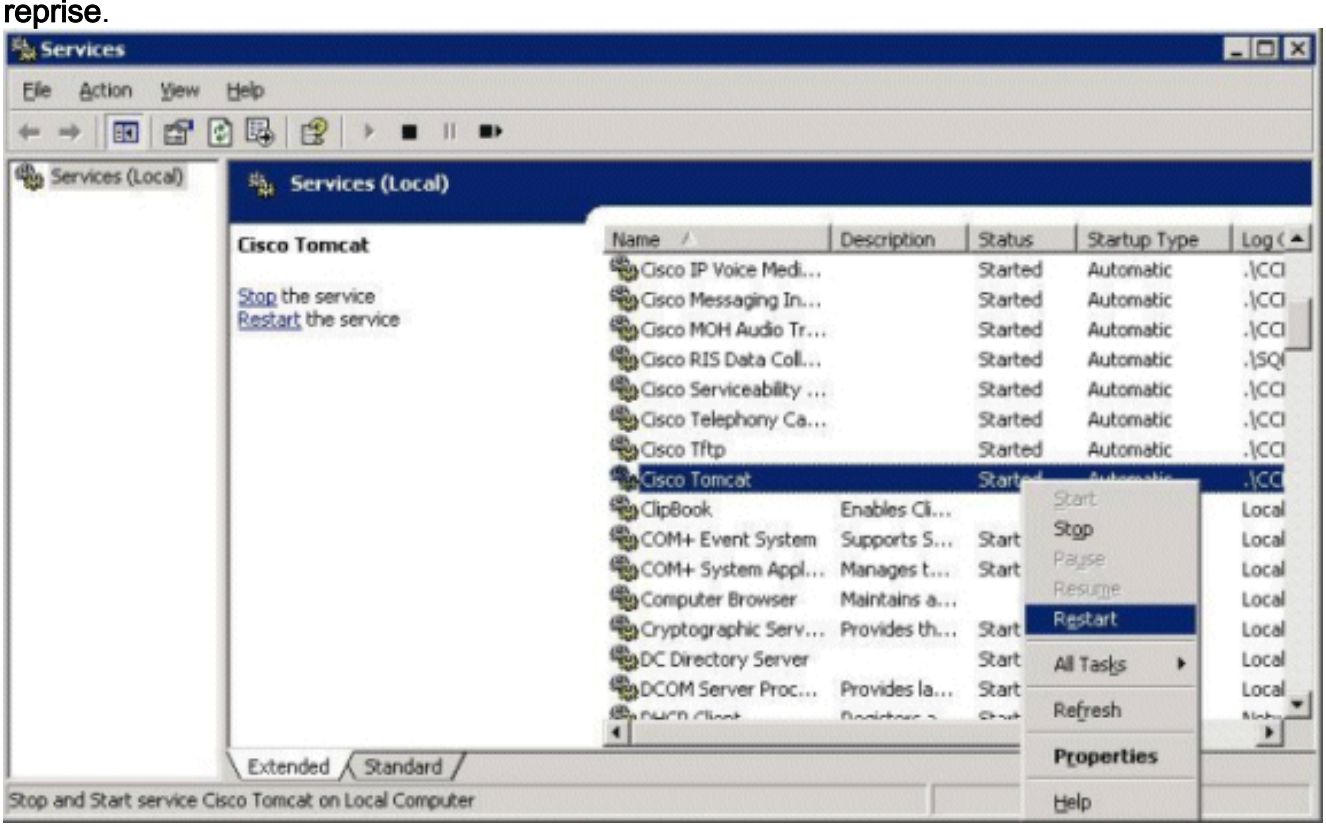
1. Choisissez **Start > Run**.
2. Entrez dans le **C de Notepad : /dcdsrvr/DirectoryConfiguration.ini et** cliquent sur OK.
3. Changez l'utilisateur, par exemple, *administrateur > ccmdiruser*.
4. Changez la valeur à la droite du `passwd= au` mot de passe chiffré que vous avez obtenu de l'outil de **PasswordUtils**.
5. Choisissez le **fichier** > la **sauvegarde**.
6. Choisissez le **fichier** > la **sortie**.



Reprise Cisco Tomcat

Suivez ces étapes pour redémarrer le service de Cisco Tomcat :

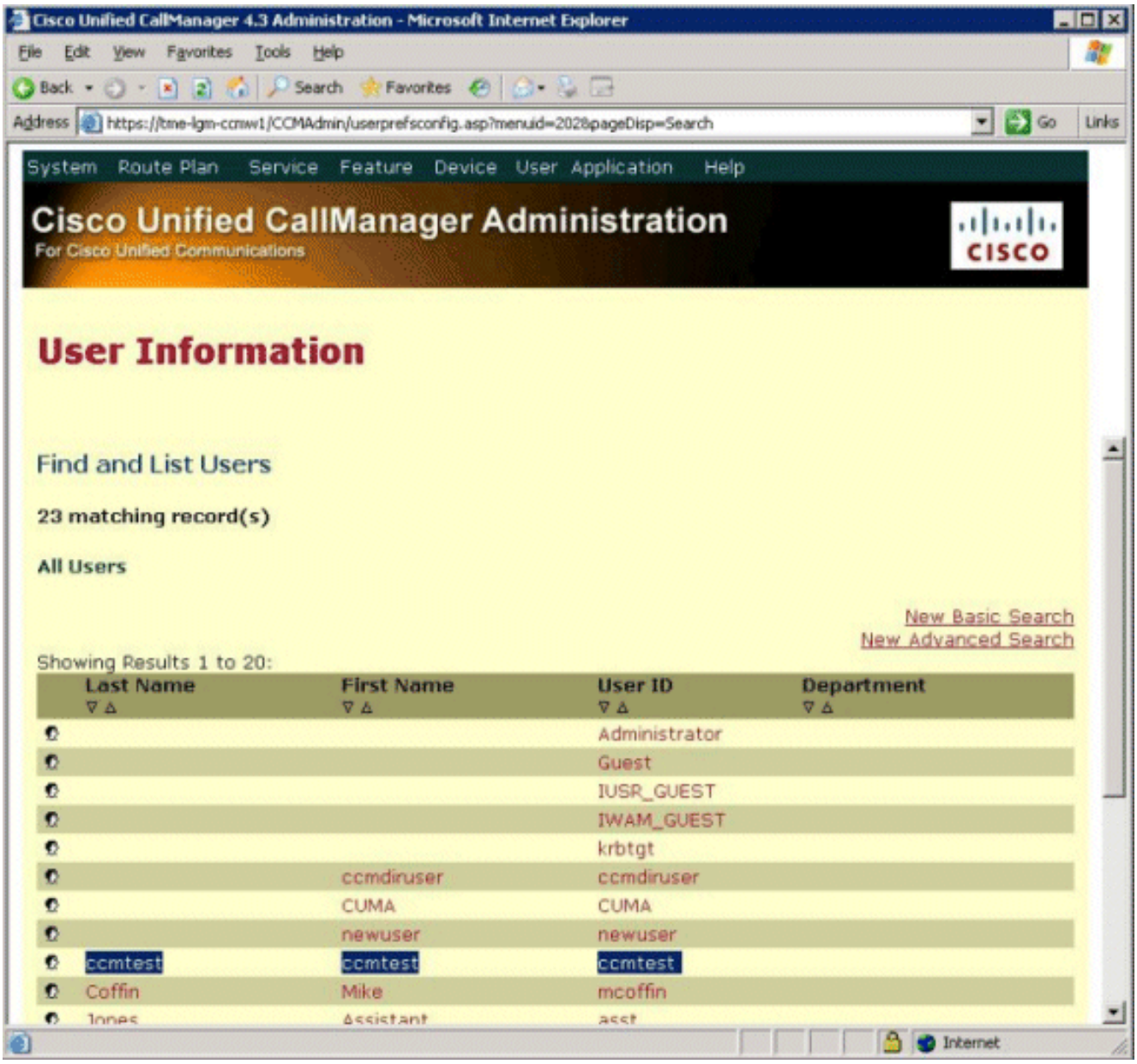
1. Choisissez le **Programs > Administrative Tools > Services**.
2. Cliquez avec le bouton droit **Cisco Tomcat** et choisissez la **reprise**.



Vérifiez que l'utilisateur ccmtest provisoire est dans le répertoire CUCM

Suivez ces étapes pour vérifier que l'utilisateur ccmtest provisoire est dans le répertoire CUCM :

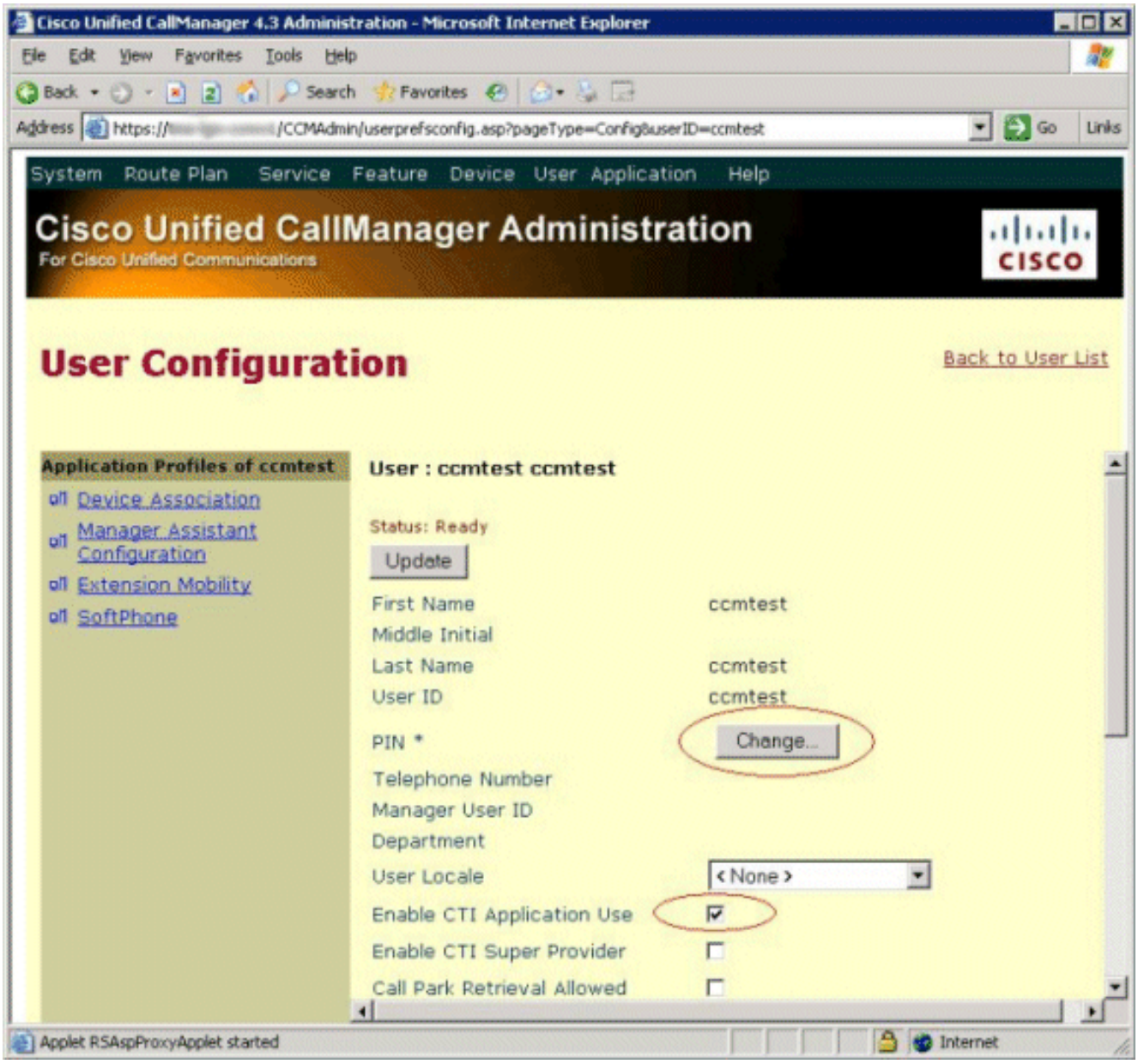
1. Des pages de gestion CUCM, choisissez l'**User > Global Directory**.
2. Appuyez sur le **bouton recherche**.
3. Assurez-vous que l'utilisateur **ccmtest** est dans la liste d'utilisateurs.



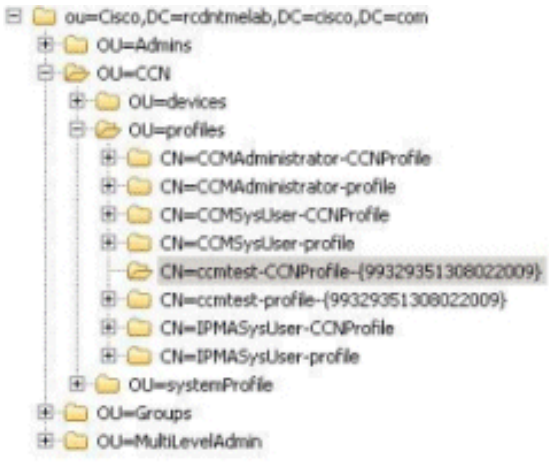
Changez le PIN de l'utilisateur ccmtest

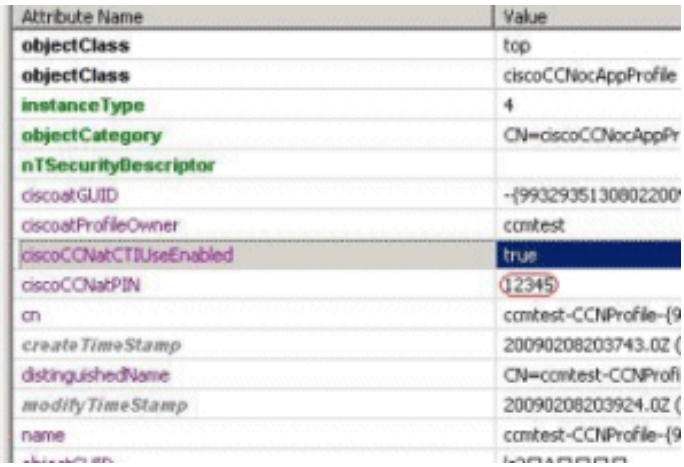
Suivez ces étapes pour changer le PIN de l'utilisateur ccmtest :

1. Choisissez **ccmtest à la** `page des informations utilisateur`.
2. Appuyez sur le bouton de **modification…**.
3. Écrivez un PIN 5-digit, par exemple, `12345`.
4. Appuyez sur la **mise à jour** et les boutons **étroits**.



5. Utilisez un navigateur de répertoire pour choisir l'**OU de Cisco**.
6. Naviguez vers **CCN** > **profils** > ccm-**test-CCNProfile**.
7. Assurez-vous que le champ de **CiscoCCNatPIN** a la nouvelle valeur.

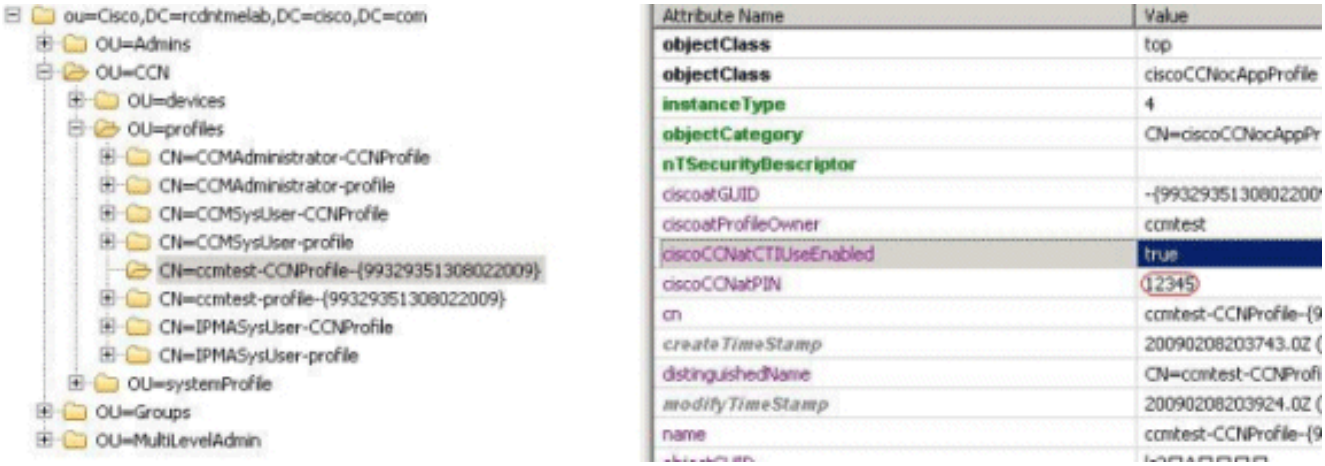




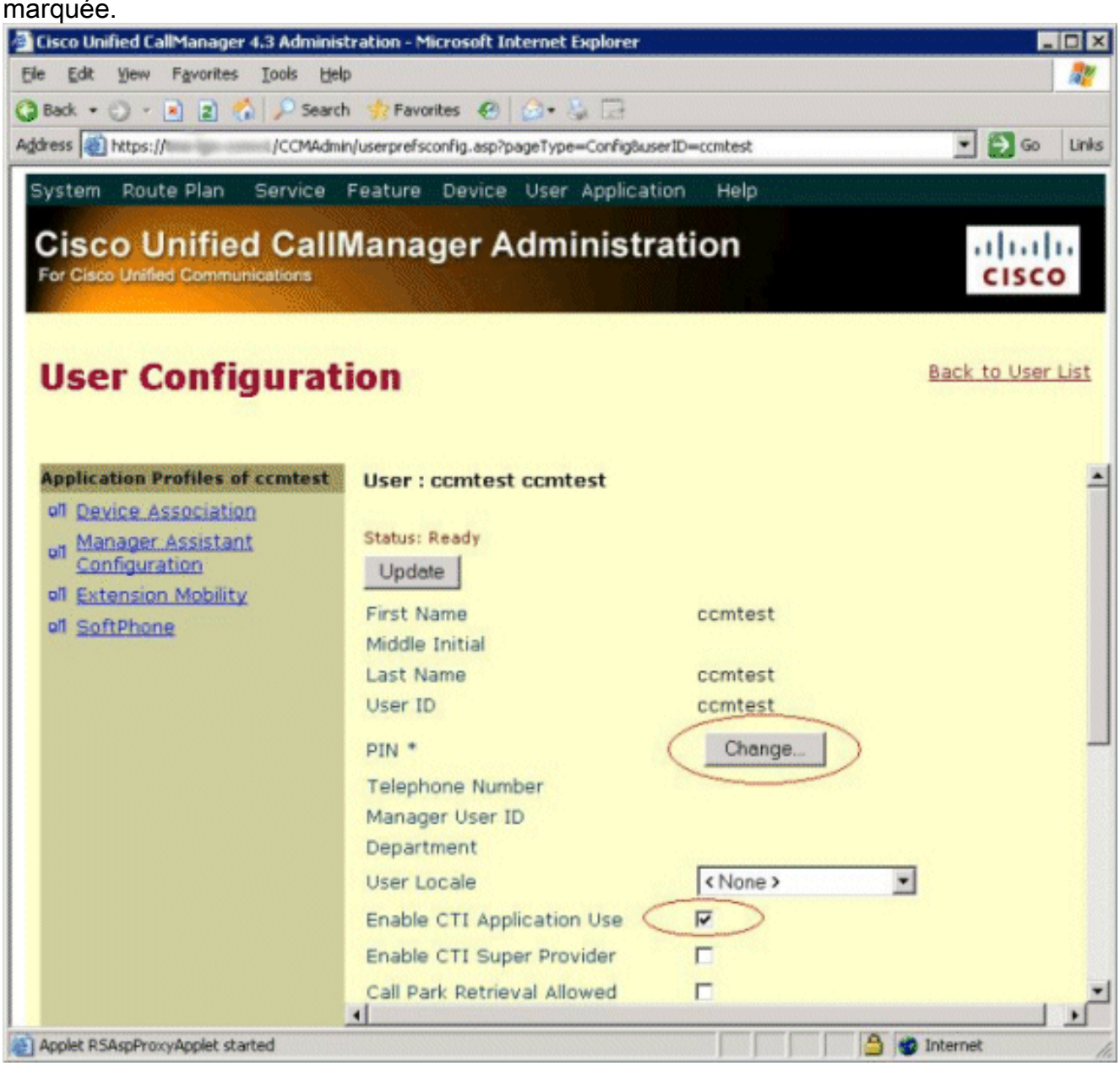
Changez le champ ciscoCCNatCTIUseEnabled

Suivez ces étapes pour changer le champ ciscoCCNatCTIUseEnabled :

1. Utilisez un navigateur de répertoire pour choisir l'**OU de Cisco**.
2. Naviguez vers **CCN > profils >** ccm-**test-CCNProfile**.
3. Modify **ciscoCCNatCTIUseEnabled pour rectifier**.



4. Régénérez la `page de configuration utilisateur` pour l'utilisateur **ccmtest**.
5. Assurez-vous que la case d'**utilisation d'application de l'enable CTI** est maintenant marquée.



Supprimez l'utilisateur ccmtest

Suivez ces étapes pour supprimer l'utilisateur ccmtest :

1. Choisissez l'**OU d'utilisateurs**.
2. Cliquez avec le bouton droit **ccmtest** et choisissez l'**effacement**.
3. Choisissez **oui** de confirmer.

Informations connexes

- Intégration de répertoire LDAP - Cisco Unified Communications SRND pour CUCM 4.x
- Installation de périphérique prêt à brancher du Répertoire actif 2000 pour le Cisco CallManager
- Guide de dépannage de l'intégration de Cisco CallManager et Active Directory
- Assistance technique concernant la technologie vocale
- Assistance concernant les produits vocaux et de communications unifiées
- Dépannage des problèmes de téléphonie IP Cisco
- Support et documentation techniques - Cisco Systems